Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Complexity 21 (2005) 230–242
Journal of COMPLEXITY
http://www.elsevier.com/locate/jco

Multi-sequences with d-perfect property ☆

Xiutao Feng,* Quanlong Wang, and Zongduo Dai

State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100039, China

Received 13 February 2004; accepted 30 April 2004

Available online 15 June 2004

Abstract

Sequences with almost perfect linear complexity profile are defined by Niederreiter (Proceedings of the Salzburg Conference 1986, Vol. 5, Teubner, Stuttgart, 1987, pp. 221–233). Xing and Lam (IEEE Trans. Inform. Theory 45 (1999) 1267; J. Complexity 16 (2000) 661) extended this concept from the case of single sequences to the case of multi-sequences and further proposed the concept of d-perfect multi-sequences. In this paper, based on the technique of m-continued fractions due to Dai et al. we investigate the property of d-perfect multi-sequences and obtain a sufficient and necessary condition of d-perfect multi-sequences. We show that d-perfect multi-sequences are not always strongly d-perfect. In particular, we give an example to disprove the conjecture proposed by Xing (2000) on d-perfect multi-sequences.

Keywords: Multi-sequences; Linear complexity profile; d-perfect; m-continued fraction

1. Introduction

Stream ciphers are based on pseudorandom key streams, i.e. specially on deterministically generated sequences of bits with acceptable properties of unpredictability and randomness [6,3]. From the cryptographic viewpoint, a useful

☆This work is partly supported by NSFC (Grant No. 60173016), and the National 973 Project (Grant No. 1999035804).

*Corresponding author.

E-mail addresses: fengxt@mails.gscas.ac.cn (X. Feng), wangquanl@mails.gscas.ac.cn (Q. Wang), yangdai@public.bta.net.cn (Z. Dai).

0885-064X/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jco.2004.04.004

measure for unpredictability is the linear complexity profile (LCP) of pseudo-random sequences. Many researchers contrived to construct pseudorandom sequences whose LCP looks like the LCP of truly random sequences. Niederreiter [4,5] introduced the concept of almost perfect linear complexity profile (PLCP). Xing and Lam [8,9] extended the concept of almost PLCP from the case of single sequences to the case of multi-sequences and further proposed the concept of d-perfect multi-sequences. In this paper, based on the technique of m-continued fractions [7,2,1], we investigate the property of d-perfect multi-sequences and obtain a sufficient and necessary condition of d-perfect multi-sequences. We show that d-perfect multi-sequences are not always strongly d-perfect and illustrate this by a counterexample.

This paper is organized as follows. In Section 2, we list the preliminary knowledge including some known results about d-perfect multi-sequences and m-continued fractions. In Section 3, we discuss d-perfect multi-sequences and get the main results. In Section 4, we further disprove the conjecture proposed by Xing on d-perfect multi-sequences with a counterexample.

2. Preliminaries

2.1. d-perfect Multi-sequences

We first introduce some notations and definitions.

Let $\mathbf{F}_q$ be a finite field with q elements. We denote by $\mathbf{F}_q^\infty$ the set of all infinite sequences of elements of $\mathbf{F}_q$. Let $\underline{s} = \{s_1, s_2, \ldots, s_n, \ldots\} \in \mathbf{F}_q^\infty$. For an arbitrary integer $n \geqslant 1$, we denote by $\underline{s}^{(n)}$ the prefix $\{s_1, s_2, \ldots, s_n\}$ of $\underline{s}$ and by $L(n)$ the linear complexity of $\underline{s}^{(n)}$ [5].

Definition 1 (Niederreiter [5]). A sequence $\underline{s} = \{s_1, s_2, \ldots, s_n, \ldots\}$ has *perfect linear complexity profile* (*PLCP*) if for all $n(\geqslant 1)$, we have

$$L(n) = \left\lfloor \frac{n+1}{2} \right\rfloor. \tag{1}$$

Consider a multi-sequence

$$S = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_m\}$$

of dimension $m > 1$, where m is a positive integer and $\underline{s}_k \in \mathbf{F}_q^\infty$, $1 \leqslant k \leqslant m$. We yet denote by $S^{(n)}$ the prefix $\{\underline{s}_1^{(n)}, \underline{s}_2^{(n)}, \ldots, \underline{s}_m^{(n)}\}$ of S and by $L(n)$ the joint linear complexity of $S^{(n)}$ [9]. Xing and Lam [8,9] investigated multi-sequences with almost PLCP and further proposed the concepts of d-perfect and perfect multi-sequences.

Definition 2 (Xing [9]). For a positive integer d, a multi-sequence $S = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_m\}$ is called *d-perfect* if

$$L(n) \geqslant \frac{m(n+1) - d}{m+1} \tag{2}$$

for all $n \geqslant 1$. In particular, S is called *perfect* if S is an m-perfect multi-sequence.

In [9], Xing got the following theorem and proposed a conjecture on d-perfect multi-sequences.

Theorem 1 (Xing [9]). *A multi-sequence $S = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_m\}$ is perfect if and only if*

$$L(n) = \left\lceil \frac{mn}{m+1} \right\rceil \tag{3}$$

for all $n \geqslant 1$.

Conjecture 1 (Xing [9]). *Let $S = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_m\}$ be a d-perfect multi-sequence of dimension m. Then*

$$\frac{m(n+1) - d}{m+1} \leqslant L(n) \leqslant \frac{mn + d}{m+1} \tag{4}$$

for all $n \geqslant 1$.

Definition 3. A multi-sequence $S = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_m\}$ of dimension m is called *strongly d-perfect* if (4) holds.

Obviously, if a multi-sequence S is strongly d-perfect, it must be d-perfect.

2.2. m-continued fractions

Let $\mathbf{Z}$ be the ring of integers. We denote by

$$\mathbf{F}_q((x^{-1})) = \left\{ \sum_{k \geqslant t} a_k x^{-k} \mid a_k \in \mathbf{F}_q, \ \ t \in \mathbf{Z} \right\}$$

the Laurent series field over $\mathbf{F}_q$. And we denote by $\mathbf{F}_q[x]$ and $\mathbf{F}_q(x)$ the polynomial ring and fraction field over $\mathbf{F}_q$, respectively. For any element $r(x) \in \mathbf{F}_q(x)$, we view $r(x)$ as an element over $\mathbf{F}_q((x^{-1}))$ according to the natural embedded method. Let $\mathbf{F}_q((x^{-1}))^m$, $\mathbf{F}_q[x]^m$ and $\mathbf{F}_q^m$ be the column vector space of dimension m over $\mathbf{F}_q((x^{-1}))$, $\mathbf{F}_q[x]$ and $\mathbf{F}_q$, respectively. For any non-zero element $A \in \mathbf{F}_q((x^{-1}))^m$, it can be written in the form of

$$A = \sum_{1 \leqslant j \leqslant m, \ k \geqslant t} a_{j,k} x^{-k} \underline{e}_j,$$

where $\underline{e}_j$ denotes the jth standard basis vector over $\mathbf{F}_q^m$, $a_{j,k} \in \mathbf{F}_q$ and t is an integer. Define $Iv(A) = (h, v)$ if $a_{h,v} \neq 0$ and $a_{j,k} = 0$ for any $j < h, k \leqslant v$ or $j > h, k < v$, and we call $Iv(A)$ the *Indexed Valuation* of A. For any two elements (h, v) and (h', v'), we

define $(h,v)<(h',v')$ if $v<v'$ or $v=v'$, $h<h'$. Clearly, the ordering defined as above on $\{1,2,\ldots,m\}\times\mathbf{Z}$ is linear [2].

Let

$$C=[\underline{a}_0,h_1,\underline{a}_1,h_2,\underline{a}_2,\ldots,h_k,\underline{a}_k,\ldots],$$

where $1\leqslant k<w$, w is a positive integer or ∞, h_k is a positive integer and $1\leqslant h_k\leqslant m$, $\underline{a}_k=(a_{k,1},a_{k,2},\ldots,a_{k,m})\in\mathbf{F}_q[x]^m$ and $\underline{a}_0=\underline{0}\in\mathbf{F}_q[x]^m$. We call C an *m-pre-continued fraction* and w the length of C. In the case when $w<\infty$, then $C=[\underline{a}_0,h_1,\underline{a}_1,h_2,\underline{a}_2,\ldots,h_{w-1},\underline{a}_{w-1}]$. We always associate C with the following quantities:

$$\begin{aligned}
&t_k=\deg(a_{k,h_k}),\\
&d_k=\sum\nolimits_{1\leqslant i\leqslant k}t_i,\quad d_0=0,\\
&v_{k,j}=\sum_{i\leqslant k,h_i=j}t_i,\quad v_{0,j}=0,\quad 1\leqslant j\leqslant m,\quad v_k=v_{k,h_k},\\
&n_k=d_{k-1}+v_k,\quad n_0=0,
\end{aligned}$$

where $\deg(a_{k,h_k})$ denotes the degree of polynomial a_{k,h_k} and $1\leqslant k<w$. By convention, $\deg(0)=-\infty$.

Definition 4 (Dai et al. [2,1]). An m-pre-continued fraction $C=[\underline{a}_0,h_1,\underline{a}_1,h_2,\underline{a}_2,\ldots,h_k,\underline{a}_k,\ldots]$ is called an *m-continued fraction* if it satisfies:

(1) $t_k\geqslant 1$, $1\leqslant k<w$;
(2) if $h_k<h_{k+1}$, then $v_{k-1,h_k}\leqslant v_{k+1}$; if $h_k>h_{k+1}$, then $v_{k-1,h_k}\leqslant v_{k+1}-1$, where $1\leqslant k<w-1$; and
(3) For $1\leqslant k<\omega$ and $1\leqslant j\leqslant m$, $j\neq h_k$,

$$\deg(a_{k,j})\leqslant\begin{cases}v_{k,j}-v_{k-1,h_k}-1, & j<h_k,\\ v_{k,j}-v_{k-1,h_k}, & j>h_k.\end{cases}$$

Remark 1. In fact, given the sequences $\{h_k\}_{k\geqslant 1}$ and $\{t_k\}_{k\geqslant 1}$, which satisfy conditions (1) and (2) for all $k\geqslant 1$, we can always construct an m-continued fraction C such that C also satisfies condition (3), e.g. let $a_{k,j}=0$ for $j(\neq h_k)$, and let a_{k,h_k} be an arbitrary polynomial with degree t_k over $\mathbf{F}_q[x]$.

In order to describe the relation of m-continued fractions and multi-sequences, we need some more notations. For a multi-sequence $S=\{\underline{s}_1,\underline{s}_2,\ldots,\underline{s}_m\}$, we identify it with $S(x)=\{\underline{s}_1(x),\underline{s}_2(x),\ldots,\underline{s}_m(x)\}$, where $\underline{s}_j(x)=\sum_{k\geqslant 1}s_{j,k}x^{-k}$ is the *generating function* of $\underline{s}_j$, $1\leqslant j\leqslant m$. We denote by $\underline{s}_j^{(n)}(x)$ the prefix $\sum_{k=1}^{n}s_{j,k}x^{-k}$ of $\underline{s}_j(x)$ and denote by $S^{(n)}(x)$ the prefix $\{\underline{s}_1^{(n)}(x),\underline{s}_2^{(n)}(x),\ldots,\underline{s}_m^{(n)}(x)\}$ of $S(x)$. Let P_h be the *permutation matrix* of order $(m+1)$ which exchanges the hth column and the $(m+1)$th column, that is,

$$P_h=(\underline{e}_1\underline{e}_2\cdots\underline{e}_{h-1}\underline{e}_{m+1}\underline{e}_{h+1}\cdots\underline{e}_m\underline{e}_h). \tag{5}$$

For a given $\underline{a} \in \mathbf{F}_q[x]^m$, we define the *$\underline{a}$-translation matrix* as below:

$$A(\underline{a}) = \begin{pmatrix} I_m & \underline{a} \\ 0 & 1 \end{pmatrix}, \tag{6}$$

where I_m is the $m \times m$ identity matrix.

Given an m-continued fraction C, we define iteratively the square matrices B_k of order $(m+1)$ over $\mathbf{F}_q[x]$ as below:

$$B_0 = I_{m+1}, \quad B_k = B_{k-1} P_{h_k} A(\underline{a}_k), \quad k \geqslant 1 \tag{7}$$

and denote by $\underline{b}_k$ the last column of B_k for $k \geqslant 0$, and let $\underline{p}_k = (p_1, p_2, \ldots, p_m) \in \mathbf{F}_q[x]^m$ and $q_k \in \mathbf{F}_q[x]$ be components of $\underline{b}_k$, as shown below:

$$\underline{b}_k = (\underline{p}_k, q_k)^\tau. \tag{8}$$

where τ means transpose. Let

$$\frac{\underline{p}_k}{q_k} = \left(\frac{p_1}{q_k}, \frac{p_2}{q_k}, \ldots, \frac{p_m}{q_k}\right)^\tau$$

and $\frac{\underline{p}_k}{q_k}$ is called the *kth approximant* of C. By Dai et al. [2], we know that $\frac{\underline{p}_k}{q_k}$ converges to an element $S(x)$ over $\mathbf{F}_q((x^{-1}))^m$ as $k \to \infty$ in the sense that for any (h, N), there exists an integer k_0, such that

$$Iv\left(S(x) - \frac{\underline{p}_k}{q_k}\right) > (h, N), \quad \forall k > k_0.$$

Moreover, we have $Iv(S(x) - \frac{\underline{p}_k}{q_k}) = (h_{k+1}, n_{k+1})$. We call C an *m-continued fraction expansion* of S. And given a multi-sequence $S = \{\underline{s}_1, \underline{s}_2, \ldots, \underline{s}_m\}$, we denote by $\mathcal{C}(S)$ the set of all m-continued fraction expansions of S. By Dai et al. [8], we know that $\mathcal{C}(S)$ is nonempty and can be got by an algorithm called *m-CF transform* (for details, see [2]).

Lemma 1 (Dai et al. [2]). *Let S be a multi-sequence of dimension m and $C \in \mathcal{C}(S)$. Then*

(1) $S^{(n_{k+1}-1)}(x) = (\frac{\underline{p}_k}{q_k})^{(n_{k+1}-1)}$ *for* $k \geqslant 1$,
(2) $L(n) = d_k$ *for* $n_k \leqslant n < n_{k+1}$ *and* $k \geqslant 1$.

By Lemma 1, we immediately get the following proposition:

Proposition 1. *Let S be a multi-sequence of dimension m* and *$C \in \mathcal{C}(S)$. Then*

(1) *S is d-perfect if and only if for all $k \geqslant 0$, we have*

$$\frac{mn_{k+1} - d}{m+1} \leqslant d_k.$$

(2) *S is strongly d-perfect if and only if for all* $k \geqslant 0$, *we have*

$$\frac{mn_{k+1} - d}{m+1} \leqslant d_k \leqslant \frac{mn_k + d}{m+1}.$$

Proof. Here we only prove item (2). Item (1) can be got directly from the proof procedure to item (2).

"⇒". Considering a given multi-sequence S, we check easily that Item (2) of Lemma 1 is also correct when $k = 0$. For an integer $k \geqslant 0$, if $n_k < n_{k+1}$, then for an arbitrary integer n, s.t. $n_k \leqslant n < n_{k+1}$, by Item (2) of Lemma 1, we have $L(n) = d_k$. Hence we can get

$$d_k = L(n_{k+1} - 1) \geqslant \frac{m((n_{k+1} - 1) + 1) - d}{m+1} = \frac{mn_{k+1} - d}{m+1}$$

and

$$d_k = L(n_k) \leqslant \frac{mn_k + d}{m+1}.$$

If $n_k = n_{k+1}$, let K_0 be an integer such that $n_k = n_{k+1} = \cdots = n_{K_0 - 1} < n_{K_0}$, similarly we have

$$d_k < d_{K_0 - 1} \leqslant \frac{mn_{K_0 - 1} + d}{m+1} = \frac{mn_k + d}{m+1},$$

and let k_0 be an integer such that $n_{k_0} < n_{k_0+1} = \cdots = n_k = n_{k+1}$, we have

$$d_k > d_{k_0} \geqslant \frac{mn_{k_0+1} - d}{m+1} = \frac{mn_{k+1} - d}{m+1}.$$

"⇐". For an arbitrary positive integer n, by Item (2) of Lemma 1, there exists an integer k, s.t. $n_k \leqslant n < n_{k+1}$ and $L(n) = d_k$. So

$$\frac{m(n+1) - d}{m+1} \leqslant \frac{m(n_{k+1}) - d}{m+1} \leqslant d_k \leqslant \frac{mn_k + d}{m+1} \leqslant \frac{mn + d}{m+1}$$

and we get the conclusion. □

3. Multi-sequences with d-perfect property

We first introduce the following two useful notations:

- $l(k,j) = \max\{i \mid h_i = j,\ 1 \leqslant i \leqslant k\}$, if such i doesn't exist, then $l(k,j) = 0$,
- $L(k,j) = \min\{i \mid h_i = j, i \geqslant k\}$, if such i doesn't exist, then $L(k,j) = 0$.

Definition 5. For a given m-continued fraction C, let

$$J = \{j \mid L(k,j) > 0,\ \text{for } \forall k \geqslant 1\}$$

and $m' = |J|$. We call m' the *characteristic* of C. C is called *non-degenerate* if $m' = m$; otherwise, C is called *degenerate*.

Definition 6. An m-continued fraction C is called *bounded* if the sequence $\{t_k\}_{k\geqslant 1}$ is bounded; otherwise, we say that it is *boundless*.

Throughout this section, we denote by c the least upper bound of the sequence $\{t_k\}_{k\geqslant 1}$ if C is bounded.

Lemma 2. *Let S be a multi-sequence of dimension m and $C\in\mathcal{C}(S)$. Then S is d-perfect if and only if*

$$t_k+\sum_{1\leqslant j\leqslant m}(v_k-v_{k,j})\leqslant d \tag{9}$$

for all $k\geqslant 1$.

Proof. Since $\sum_{1\leqslant j\leqslant m} v_{k,j}=d_k$, we have

$$\begin{aligned} t_k+\sum_{1\leqslant j\leqslant m}(v_k-v_{k,j}) &= t_k+mv_k-d_k=t_k+m(n_k-d_{k-1})-d_k\\ &= mn_k-(m+1)d_{k-1}. \end{aligned}$$

By Proposition 1, we can get the conclusion directly. □

In order to evaluate $v_{k,j}-v_k$, we consider the sequence $\{(j_i,k_i)\}_{0\leqslant i\leqslant\tau}$, which is defined iteratively as follows: Initiate $j_0=j$ and $k_0=l(k,j_0)$. Assume (j_i,k_i) is defined. If $j_i=h_k$, let $\tau=i$, the procedure stops; if $j_i\neq h_k$, let $j_{i+1}=h_{k_i+1}$, and $k_{i+1}=l(k,j_{i+1})$. It is clear that $j_i\neq j_s$ for $\forall i\neq s$, hence τ exists, and $\tau<m$.

Lemma 3. *Let the sequence $\{(j_i,k_i)\}_{0\leqslant i\leqslant\tau}$ be defined as above. Then*

$$v_{k,j}-v_k\leqslant t_{k_0}-t_k+\sum_{s=0}^{\tau-1}t_{k_s+1}. \tag{10}$$

Proof. By the second condition of m-continued fractions, we have $v_{k-1,h_k}\leqslant v_{k+1}$, that is

$$v_k-v_{k,h_{k+1}}\leqslant t_k+t_{k+1}.$$

Note that $h_{k_i+1}=j_{i+1}=h_{k_{i+1}}$, $v_{k,j_i}=v_{k_i}$ and $v_{k_{i+1}}=v_{k_{i+1}-1,j_{i+1}}+t_{k_{i+1}}$, we have

$$v_{k,j_i}-v_{k,j_{i+1}}=v_{k_i}-v_{k_{i+1}}=v_{k_i}-v_{k_{i+1}-1,j_{i+1}}-t_{k_{i+1}}.$$

By $k_i+1\leqslant k_{i+1}$ and $v_k-v_{k,h_{k+1}}\leqslant t_k+t_{k+1}$, we get

$$v_{k,j_i}-v_{k,j_{i+1}}=v_{k_i}-v_{k_{i+1}-1,h_{k_i+1}}-t_{k_{i+1}}\leqslant v_{k_i}-v_{k_i,h_{k_i+1}}-t_{k_{i+1}}\leqslant t_{k_i}+t_{k_i+1}-t_{k_{i+1}}.$$

So

$$v_{k,j} - v_k = \sum_{s=0}^{\tau-1} (v_{k,j_s} - v_{k,j_{s+1}}) \leqslant \sum_{s=0}^{\tau-1} (t_{k_s} + t_{k_s+1} - t_{k_{s+1}})$$
$$= t_{k_0} - t_k + \sum_{s=0}^{\tau-1} t_{k_s+1}. \qquad \square$$

Lemma 4. *If an m-continued fraction C is bounded and non-degenerate, then*

$$|v_k - v_{k,j}| \leqslant mc \tag{11}$$

for all $k \geqslant 1$ *and* $1 \leqslant j \leqslant m$.

Proof. When $j = h_k$, it is trivial and we will consider the case of $j \neq h_k$. By Lemma 3, for $k \geqslant 1$ and $1 \leqslant j \leqslant m$, $j \neq h_k$, we have

$$v_{k,j} - v_k \leqslant t_{k_0} - t_k + \sum_{s=0}^{\tau-1} t_{k_s+1} \leqslant mc - t_k < mc.$$

Similarly, set $K = L(k,j)$. Since C is non-degenerate, $K > k$. Note that $v_{k,j} = v_{K-1,j} = v_K - t_K$, so

$$v_k - v_{k,j} = v_k - v_{K-1,j} \leqslant v_{K,h_k} - v_K + t_K \leqslant mc.$$

Synthesize the above two aspects and we can get the desired result. $\square$

We now establish the main result of a sufficient and necessary condition on d-perfect multi-sequences.

Theorem 2. *Let S be a multi-sequence of dimension m and* $C \in \mathcal{C}(S)$. *Then the following conditions are equivalent to each other*:

(1) *S is d-perfect for some constant positive integer d*,
(2) *C is bounded and non-degenerate*,
(3) *S is strongly d′-perfect for some constant positive integer d′*.

Proof. "1 ⇒ 2." We first prove that C is bounded. For simplification, let $t_0 = 0$. In fact, we check easily that Inequality (9) is also correct when $k = 0$. For every $k \geqslant 1$ and $1 \leqslant h \leqslant m$, note that $v_{l(k,h)} = v_{k,h}$ and $v_{l(k,h),j} \leqslant v_{k,j}$ $(1 \leqslant j \leqslant m, j \neq h)$, by Lemma 2, we have:

$$d \geqslant t_{l(k,h)} + \sum_{1 \leqslant j \leqslant m} (v_{l(k,h)} - v_{l(k,h),j}) \geqslant t_{l(k,h)} + \sum_{1 \leqslant j \leqslant m} (v_{k,h} - v_{k,j}).$$

Add two sides of the above m inequalities (h from 1 to m) together, respectively, and we can get

$$md \geqslant \sum_{h=1}^{m} t_{l(k,h)} \geqslant t_k$$

for every $k \geqslant 1$. Second, if C is degenerate, let m' and J be defined as in Definition 5, then $m' < m$. Consider sufficiently large k's, i.e. $k \gg k_0 = \min\{n \mid L(n,j) = 0,\ j \notin J\}$, and we

$$\begin{aligned} d &\geqslant t_k + \sum_{1 \leqslant j \leqslant m} (v_k - v_{k,j}) = t_k + \sum_{j \in J} (v_k - v_{k,j}) + \sum_{j \notin J} (v_k - v_{k,j}) \\ &= t_k + \sum_{j \in J} (v_k - v_{k,j}) + (m - m')v_k - \sum_{j \notin J} v_{k_0,j}. \end{aligned} \tag{12}$$

By Lemma 4, we have

$$\left| \sum_{j \in J} (v_k - v_{k,j}) \right| \leqslant \sum_{j \in J} |v_{k,j} - v_k| \leqslant (m' - 1)mc.$$

Since only one term $(m - m')v_k$ in the right side of (12) is infinite, this will lead to a contradiction.

"2 $\Rightarrow$ 3." By Lemma 4, we have

$$|d_k - mv_k| = \left| \sum_{1 \leqslant j \leqslant m,\ j \neq h_k} (v_{k,j} - v_k) \right| \leqslant \sum_{1 \leqslant j \leqslant m, j \neq h_k} |v_{k,j} - v_k| \leqslant (m-1)mc.$$

Set $d' = m^2 c$, then

$$\begin{aligned} mn_{k+1} - (m+1)d_k &= m(d_k + v_{k+1}) - (m+1)d_k \\ &= mv_{k+1} - d_k = t_{k+1} + (mv_{k+1} - d_{k+1}) \\ &\leqslant c + m(m-1)c < d' \end{aligned} \tag{13}$$

and

$$\begin{aligned} (m+1)d_k - mn_k &= (m+1)d_k - m(d_k + v_k - t_k) \\ &= mt_k + (d_k - mv_k) \\ &\leqslant mc + m(m-1)c \leqslant d'. \end{aligned} \tag{14}$$

Synthesize the above two inequalities and get that S is strongly d'-perfect.

"3 $\Rightarrow$ 1." It is trivial. $\square$

Remark 2. Though the fact that a multi-sequence S is d-perfect implies that there is a constant d' such that S is strongly d'-perfect, d' is not usually equal to d. Let

$$d_0 = \max_{k \geqslant 1} \left\{ t_k + \sum_{1 \leqslant j \leqslant m} (v_k - v_{k,j}) \right\}$$

and

$$d_1 = \max_{k \geqslant 1} \left\{ mt_k + \sum_{1 \leqslant j \leqslant m} (v_{k,j} - v_k) \right\}.$$

Then for a positive integer d, a sufficient and necessary condition that S is d-perfect is that $d \geqslant d_0$. If $d \geqslant d_1$, then S is also strongly d-perfect. If $d_0 \leqslant d < d_1$, then S is only d-perfect but not strongly d-perfect.

In particular, for perfect multi-sequences, we have:

Theorem 3. *Let S be a multi-sequence of dimension m and $C \in \mathcal{C}(S)$. Then S is perfect if and only if*

(1) *for all $k \geqslant 1$, $t_k = 1$, and*
(2) *for $\forall t \geqslant 0$, $h_{tm+1}, h_{tm+2}, \ldots, h_{tm+m}$ is pairwise unequal.*

Proof. "$\Rightarrow$." First, we prove that it is correct for $1 \leqslant k \leqslant m$ and $t = 0$. When $k = 1$, $mt_1 \leqslant d = m$, so $t_1 = 1$. Suppose that when $k \leqslant k_0 (k_0 < m)$, $t_k = 1$ and $l(k-1, h_k) = 0$. If $l(k, h_{k+1}) > 0$, then

$$\begin{aligned} m &\geqslant t_{k+1} + \sum_{1 \leqslant j \leqslant m,\ j \neq h_{k+1}} (v_{k+1} - v_{k+1,j}) \\ &= t_{k+1} + (k-1)t_{k+1} + (m-k)(t_{k+1}+1) \\ &> mt_{k+1} \geqslant m. \end{aligned}$$

This leads to a contradiction. So $l(k, h_{k+1}) = 0$ and

$$t_{k+1} + \sum_{1 \leqslant j \leqslant m,\ j \neq h_{k+1}} (v_{k+1} - v_{k+1,j}) = mt_{k+1} - k + 1 \leqslant m.$$

Therefore $t_{k+1} \leqslant \frac{m+k-1}{m} < 2$, it implies that $t_{k+1} = 1$.

Second, the process of the case of $k_0 m + 1 \leqslant k \leqslant k_0 m + m$ and $t = k_0 (\geqslant 1)$ is the same as the process of the case of $k_0 = 0$. It is because: for every $1 \leqslant j \leqslant m$, we have $v_{k_0 m, j} = k_0$. So the portion of each $v_{k_0 m + i, j}$ before $k_0 m$ is vanished when it subtracts from others by Formula (9) and it comes back to the state of $k_0 = 0$. Thus we immediately get the desired conclusion.

"$\Leftarrow$." We can check Inequality (9) directly and get easily that S is m-perfect. So S is perfect. $\square$

Remark 3. By Theorem 3, we can get the conclusion that multi-sequences with PLCP are weak and easily predictable. It is a natural generalization of Theorem 2 in [5, section 4] from the case of single sequences to the case of multi-sequences.

Remark 4. By Theorem 3, if $n = n_{tm+j} (t \geqslant 0$ *and* $1 \leqslant j \leqslant m)$, we have $n = d_{tm+j} + v_{tm+j-1, h_{tm+j}} = tm + j + t$ and $L(n) = d_{tm+j} = tm + j$. It directly leads to Theorem 1.

4. A counterexample

In this section, we present an example to illustrate that d-perfect multi-sequences are not always strongly d-perfect. So, the conjecture proposed by Xing on d-perfect multi-sequences is not correct.

Example. Let

$$C = [\underline{0}, h_1, \underline{a}_1, h_2, \underline{a}_2, \ldots, h_k, \underline{a}_k, \ldots],$$

where $\underline{a}_k = (a_{k,1}, a_{k,2}, \ldots, a_{k,m}) \in \mathbf{F}_q[x]^m$, $m \geqslant 2$, such that

$$a_{k,j} = \begin{cases} x^{t_k}, & j = h_k \\ 0, & j \neq h_k \end{cases}$$

and

$$t_k = \begin{cases} 1, & k = (2t+1)m, \\ 3, & k = (2t+2)m, \\ 2, & \text{others} \end{cases}$$

and $h_{tm+j} = j$, $t \geqslant 0$, $1 \leqslant j \leqslant m$.

Proposition 2. *Let C be defined as above. Then C is an m-continued fraction. And let $\frac{\underline{p}_k}{q_k}$ be the kth approximant of C and $S(x) = \lim_{k\to\infty} \frac{\underline{p}_k}{q_k}$. Then S is $(2m+1)$-perfect but not strongly $(2m+1)$-perfect.*

Clearly, by the definitions of B_k, $\underline{p}_k$ and q_k, we have

$$\underline{p}_0 = \underline{\mathbf{0}}, \quad \underline{p}_k = \begin{cases} \underline{p}_{k-m-1} + x^{t_k}\underline{p}_{k-1}, & k > m \\ \underline{e}_k + x^{t_k}\underline{p}_{k-1}, & 1 \leqslant k \leqslant m \end{cases}$$

and

$$q_0 = 1, \quad q_k = \begin{cases} q_{k-m-1} + x^{t_k} q_{k-1}, & k > m, \\ x^{t_k} q_{k-1}, & 1 \leqslant k \leqslant m. \end{cases}$$

In particular, for $m = 2$ and $\underline{a}_k \in \mathbf{F}_2[x]^2$, note that $n_{4k+1} = 12k$, by Item (1) of Lemma 1, we have

$$S^{(12k-1)}(x) = \left(\frac{\underline{p}_{4k}}{q_{4k}}\right)^{(12k-1)}.$$

Let $S(x) = (\underline{s}_1(x), \underline{s}_2(x))$ and take $k = 7$. Then we have

$$\underline{s}_1^{(83)} = 01000010000111001011111001010011001111101110101011101001100$$
$$011011100011111111101111,$$

and

$$\underline{s}_2^{(83)} = 00100001100010110111110001110101010001010001001010001100001$$
$$0100000111010000000111110.$$

Below, we provide a brief proof of Proposition 2.

Proof. First, we check easily that C is an m-continued fraction. In fact, for $t \geqslant 0,\ 1 \leqslant i, j < m$, we have

$$v_{tm+i,j} = \begin{cases} 2t, & i < j \\ 2(t+1), & i \geqslant j \end{cases}$$

and

$$v_{k,m} = \begin{cases} 4t+1, & k = (2t+1)m, \\ 4(t+1), & k = (2t+2)m. \end{cases}$$

Then

$$v_{k+1} - v_{k-1,h_k} = \begin{cases} 1, & k = (2t+1)m - 1, \\ 4, & k = (2t+1)m, \\ 5, & k = (2t+2)m, \\ 2, & \text{others.} \end{cases}$$

Thus $v_{k+1} - v_{k-1,h_k} \geqslant 1$ and C is an m-continued fraction.

Second, we have

$$t_k + \sum_{1 \leqslant j \leqslant m} (v_k - v_{k,j}) = \begin{cases} 2(m-i+1), & k = (2t+1)m + i,\ 1 \leqslant i \leqslant m-1, \\ 2(m-i+1)+1, & k = (2t+2)m + i,\ 1 \leqslant i \leqslant m-1, \\ 2-m, & k = (2t+1)m, \\ 0, & k = (2t+2)m. \end{cases}$$

Thus we immediately get

$$t_k + \sum_{1 \leqslant j \leqslant m} (v_k - v_{k,j}) \leqslant 2m + 1 = d,$$

and by Lemma 2, S is $(2m+1)$-perfect. But when $k = (2t+2)m$, we have

$$(m+1)d_k - mn_k = mt_k + \sum_{1 \leqslant j \leqslant m} (v_{k,j} - v_k) = 3m > 2m + 1 = d.$$

Therefore S is not strongly $(2m+1)$-perfect. □

Acknowledgments

The authors gratefully acknowledge the anonymous referees, whose comments helped to improve the presentation.

References

[1] Z. Dai, K. Wang, D. Ye, *m*-continued fraction expansions of multi-Laurent series, Adv. Math. (China) 33 (2004) 246–248.
[2] Z. Dai, K. Wang, D. Ye, Multidimensional Continued Fraction and Rational Approximation, http://arxiv.org/abs/math.NT/0401141.
[3] R. Lidl, H. Niederreiter, Introduction to Finite Fields and their Applications, Cambridge University Press, Cambridge, 1986.
[4] H. Niederreiter, Continued fractions for formal power series, pseudorandom numbers, and linear complexity of sequences, Contributions to General Algebra, Proceedings of the Salzburg Conference 1986, Vol. 5, Teubner, Stuttgart, 1987, pp. 221–233.
[5] H. Niederreiter, Sequences with almost perfect linear complexity profile, Advances in Cryptology-EUROCRYPT' 87, Lecture Notes in Computer Science, Vol. 304, Springer, Berlin, 1988, pp. 37–51.
[6] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer, Berlin, 1986.
[7] H. Stark, An Introduction to Number Theory, MIT Press, Cambridge, MA, 1979.
[8] C. Xing, K.Y. Lam, Sequences with almost perfect linear complexity profiles and curves over finite fields, IEEE Trans. Inform. Theory 45 (1999) 1267–1270.
[9] C. Xing, Multi-sequences with almost perfect linear complexity profile and function fields over finite fields, J. Complexity 16 (2000) 661–675.